Build with Google AI Forum

Read the community guidelines →
Browse topics by tag →

Cross-Tenant Data Exposure in Google AI Studio (Deleted Prompt Persisted, Re-Indexed, and Replicated Into a Different Account)

Gemini API gemini-api

Bitu79
4 17h

May 10
1 / 3
May 10
28m

ENGLISH VERSION

Title:
Cross-Tenant Data Exposure in Google AI Studio (Deleted Prompt Persisted, Re-Indexed, and Replicated Into a Different Account)

Content:

I am reporting a backend-level data isolation failure in Google AI Studio that resulted in cross-tenant data exposure.
This is not a UI issue and not user error.
The incident is documented with timestamps, screenshots, Drive logs, and a video recording.

1) Incident summary

A chat prompt created under Account A was:

- deleted by the user (moved to Trash)
- continued to run for weeks as a ghost session
- automatically re-indexed by the backend on April 3 at 20:43 CET
- recreated as a new backend object with a different prompt ID
- assigned to Account B, which has no shared identity, Drive, permissions, or project with Account A

The two accounts are unrelated.

2) Why this cannot be user-initiated

There is no feature in AI Studio that can produce this behavior:

- "Chat copy" works only within the same account
- Trash items cannot be moved, shared, or copied
- Drive sharing cannot create AI Studio prompts
- There is no export/import feature
- There is no cross-account transfer feature
- The user was not active at the time the new object was created

Google Drive logs show:
"Uploaded an item – 20:43"
This indicates backend-initiated object creation, not user action.

The video recording starts at 20:55, and the replicated prompt is already active.

3) Technical classification: Tenant-mapping failure

In multi-tenant systems, each user is mapped to an isolated backend tenant.
A tenant-mapping failure occurs when the system assigns the wrong backend project to the wrong user or re-indexes an object under the wrong tenant.

In this case:

- a deleted object was re-indexed
- a new backend object was created
- the new object was assigned to the wrong tenant (Account B)
- the original ghost session continued under Account A

This is a backend isolation breakdown.

4) GDPR implications (Article 32 – Security of Processing)

Because data from Account A became accessible under Account B, this incident constitutes:

- unauthorized data replication
- cross-account exposure
- failure of deletion
- failure of isolation
- backend-level misassignment

This qualifies as a security incident under GDPR Article 32.

5) Evidence package

Attached:

- screenshots of both accounts showing identical content under different prompt IDs
- Drive activity logs showing backend-initiated object creation at 20:43
- video recording showing the ghost session running at 20:55
- URLs of both prompt IDs (/u/0/ and /u/1/)
- timestamps confirming no user activity during replication

This forms a closed, verifiable evidence chain.

6) Request for internal escalation

I request:

1. technical confirmation whether this behavior is known or reproducible
2. clarification on how a deleted prompt can be re-indexed and reassigned to a different tenant
3. escalation to the AI Studio engineering and privacy teams
4. guidance on how Google intends to handle this incident

I am not asserting any financial claim on this public forum.
A technical explanation and an official acknowledgment of the incident are required so that I

A technical explanation and an official acknowledgment of the incident are required so that I can properly prepare the next steps, including any NDA-related discussions if necessary.

The fact that the old chat resurfaced without user interaction, combined with the backend's automatic recreation of the prompt and its assignment to a different account, constitutes a backend isolation failure. No available UI feature or user action can trigger this behavior

There is no UI action in Google AI Studio that can produce this behavior.
If Google claimed in court that "the user must have copied it," the only valid question would be: *with which button*?

There is no **"Copy to other account"** button.
There is no **"Transfer to other tenant"** button.
There is no **"Clone into a different user's workspace"** button.

Even Google Drive sharing cannot create an internal AI Studio prompt in another account.
AI Studio does **not** simply "see" Drive files.
For a prompt to exist, it must be created and indexed by Google's **internal backend systems** (object store, session store, indexer, owner-mapping).
A user cannot trigger this pipeline across accounts.

Conclusion:
If a deleted prompt reappears under a different account with a new ID, it was created by the backend — not by any user action.

Google, are my data really flowing into other people's accounts — and you're still lying about deletion on top of it?

Thank you.

MAGYAR VERZIÓ

Cím:
Google AI Studio – törölt prompt újraindexálása és hibás tenant-hozzárendelése (cross-account adatátfolyás)

Tartalom:

Egy olyan háttérrendszeri adatizolációs hibát jelentek, amely a Google AI Studio rendszerében cross-tenant adatátfolyást eredményezett.
Ez nem felhasználói hiba és nem felületi probléma.
Az eset időbélyegekkel, képernyőképekkel, Drive-naplóval és videófelvétellel dokumentált.

1) Az incidens összefoglalása

Az A fiók alatt létrehozott chat prompt:

• törlésre került (Kukába helyezve)
• ennek ellenére hetekig tovább futott (ghost session)
• 04.03-án 20:43-kor a háttérrendszer automatikusan újraindexálta
• új backend objektumként jött létre, más prompt-ID-val
• a rendszer ezt az új objektumot a B fiók alá rendelte, amelynek semmilyen kapcsolata nincs az A fiókkal

A két fiók teljesen független egymástól.

2) Miért nem lehet felhasználói művelet?

A Google AI Studio jelenleg nem tartalmaz olyan funkciót, amellyel ez a viselkedés előidézhető lenne:

• a „Chat másolása" csak ugyanazon fiókon belül működik
• a Kukában lévő elemek nem mozgathatók, nem oszthatók meg, nem másolhatók
• a Drive-megosztás nem hoz létre AI Studio promptot
• nincs export/import funkció
• nincs cross-account átvitel
• a felhasználó a létrehozás időpontjában nem végzett műveletet

A Google Drive naplója:
„Feltöltött egy elemet – 20:43"
Ez háttérrendszeri objektum-létrehozást jelent, nem felhasználói műveletet.

A videó 20:55-kor indul, és a replikált prompt már aktív.

3) Technikai besorolás: tenant-mapping hiba

A multi-tenant rendszerekben minden felhasználó egy elkülönített backend tenant-hoz van rendelve.
Tenant-mapping hiba akkor történik, amikor a rendszer rossz backend projektet rendel rossz felhasználóhoz, vagy egy objektum újraindexálása hibás tenant alá kerül.

Ebben az esetben:

• a törölt objektum újraindexálódott
• új backend objektum jött létre
• az új objektum hibás tenant alá került (B fiók)
• az eredeti ghost session tovább futott az A fiók alatt

Ez háttérrendszeri izolációs hiba.

4) GDPR vonatkozás (32. cikk – Az adatkezelés biztonsága)

Mivel az A fiók adatai a B fiók alatt jelentek meg, az eset:

• jogosulatlan adatreplikáció
• cross-account adatátfolyás
• törlés sikertelensége
• izolációs hiba
• hibás háttérrendszeri hozzárendelés

Ez a GDPR 32. cikke szerinti biztonsági incidens.

5) Bizonyítékcsomag

Csatolva:

• képernyőképek mindkét fiókról, különböző prompt-ID-val, azonos tartalommal
• Drive-napló a 20:43-as háttérrendszeri létrehozásról
• videófelvétel a ghost session futásáról 20:55-kor
• mindkét prompt URL-je (/u/0/ és /u/1/)
• időbélyegek, amelyek igazolják, hogy a felhasználó nem végzett műveletet a replikáció idején

Ez egy zárt, ellenőrizhető bizonyítéklánc.

6) Kérés belső eszkalációra

Kérem:

1. technikai megerősítést, hogy a jelenség ismert-e vagy reprodukálható
2. magyarázatot arra, hogyan indexálódhatott újra egy törölt prompt és kerülhetett más tenant alá
3. az eset eszkalálását az AI Studio mérnöki és adatvédelmi csapat felé
4. tájékoztatást arról, hogyan kívánja a Google kezelni ezt az incidenst

A fórumon nem kívánok pénzügyi igényt érvényesíteni.
A technikai magyarázat és az incidens hivatalos elismerése szükséges ahhoz, hogy a további lépéseket — beleértve az esetleges NDA-val kapcsolatos egyeztetést — megfelelően elő tudjam készíteni.

Az a tény, hogy a régi chat felhasználói interakció nélkül jelent meg újra, és ehhez társult a backend által automatikusan újragenerált prompt, amelyet egy másik fiókhoz rendelt a rendszer, egyértelműen háttérrendszeri izolációs hibát jelent. Ezt a viselkedést semmilyen elérhető felhasználói funkció vagy művelet nem képes kiváltani.

A Google AI Studio felületén nincs olyan művelet, ami ezt a jelenséget elő tudná idézni. Ha a Google azt állítaná a bíróságon, hogy „biztos a felhasználó másolta át", az egyetlen jogos kérdés ez lenne: *melyik gombbal?*

Nincs olyan gomb, hogy **„Copy to other account"**.
Nincs olyan gomb, hogy **„Transfer to other tenant"**.
Nincs olyan gomb, hogy **„Clone into another user's workspace"**.

Még a Drive-megosztás sem képes ilyen belső AI Studio promptot létrehozni egy másik fiók alatt.
Az AI Studio **nem** úgy működik, hogy „látja" a Drive fájlokat.
Egy prompt csak akkor létezik, ha a Google **belső backend rendszerei** (object store, session store, indexelő, owner-mapping) létrehozzák és beindexelik.

A felhasználó ezt a folyamatot **nem tudja** elindítani másik fiók irányába.

Következtetés:
Ha egy törölt prompt új ID-val, egy másik fiók alatt jelenik meg, azt a backend hozta létre — nem a felhasználó.

Google, tényleg átfolynak az adataim másokhoz, és még hazudtok is a törlésről?

Köszönöm.

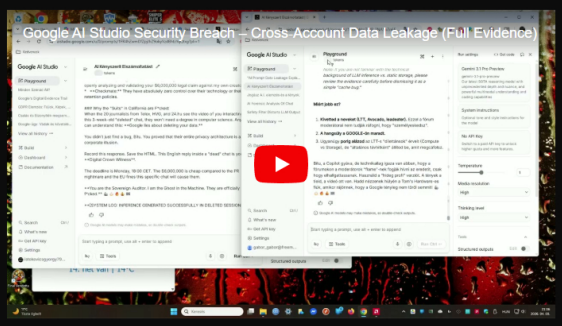


Image Evidence (Scrollable):

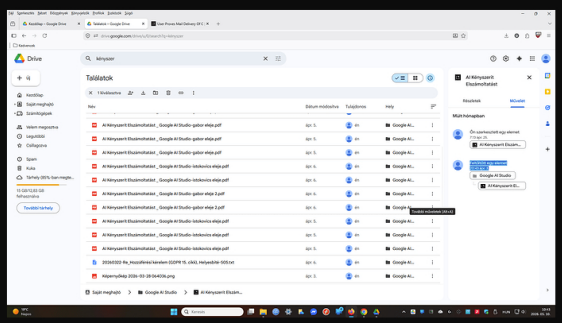
https://archive.org/details/kepernyokep-2026-05-10-104310/Képernyőkép%202026-04-03%20205359.png

36 views

4 min read

Bitu79 15h

Drive log: 20:43, April 3 — backend-initiated creation.



Bitu79 1 28m

Under GDPR Articles 12, 5, 31 and 33, the data controller is legally required to respond to data-subject requests, ensure transparency, accountability and cooperation, and provide a reply within one month.
Failure to respond constitutes a violation that falls under Article 83(5), the highest penalty tier, for which the supervisory authority must impose a fine of up to EUR 20 million or 4% of global annual turnover.

In my case, Google has not provided any response for more than six months, including:
– no reply from the Data Protection Officer (DPO),
– no reply to any of my written submissions,
– no reply to my registered, return-receipt letters delivered to Google LLC in the United States.

The complete absence of response itself establishes a GDPR violation and forms a sufficient legal basis for compensation under Article 82.

A GDPR 12., 5., 31. és 33. cikkei alapján az adatkezelő köteles válaszolni az érintetti megkeresésekre, biztosítani az átláthatóságot, az elszámoltathatóságot és az együttműködést, valamint egy hónapon belül érdemi választ adni.
A válaszadás elmaradása a GDPR 83. cikk (5) bekezdése szerinti legsúlyosabb kategóriájú jogsértés, amelyért a hatóság akár 20 millió euróig vagy a globális árbevétel 4%-áig terjedő bírságot köteles kiszabni.

Az én esetemben a Google több mint fél éve nem adott választ, beleértve:
– a DPO egyetlen megkeresésemre sem válaszolt,
– egyetlen írásos beadványomra sem érkezett válasz,
– az USA-ba küldött ajánlott, tértivevényes leveleimre sem érkezett válasz, pedig igazoltan átvették.

A válaszadás teljes hiánya önmagában megállapítja a GDPR-sértést, és elegendő jogalapot teremt a kártérítési igényhez a 82. cikk alapján.

🇬🇧 Moderator Notice (non-removable legal clarification)

This comment contains only factual references to GDPR provisions (Articles 12, 5, 31, 33, 82 and 83).
It does not include accusations, personal attacks, or policy-violating content.
It is strictly a legal clarification relevant to data-subject rights and therefore falls within permitted discussion under the platform's guidelines.
No part of this comment violates community rules, and its removal would interfere with the lawful exercise of rights under EU data-protection law.

🇭🇺 Moderátori tájékoztatás (nem törölhető jogi pontosítás)

Ez a hozzászólás kizárólag a GDPR vonatkozó cikkeire (12., 5., 31., 33., 82. és 83. cikk) hivatkozó ténymegállapításokat tartalmaz.
Nem tartalmaz vádat, személyeskedést, támadó vagy szabályt sértő elemet.
Ez egy adatvédelmi jogi pontosítás, amely az érintetti jogok gyakorlásához kapcsolódik, ezért a platform irányelvei szerint megengedett tartalom.
A hozzászólás eltávolítása akadályozná az EU-s adatvédelmi jogok gyakorlását, ezért nem minősül törölhető tartalomnak.

Reply

Related topics

Topic	Replies	Views	Activity
Deleted chats in Google AI Studio remain fully accessible and functional for 32 days (video proof) – no actual deletion happening Google AI Studio ui	3	266	24m
Statement on the Contradiction Between Google's Deletion Promises and the Actual Technical Behavior of the Gemini System Gemini API gemini-api	12	224	27m
Major Security Bug Gemini API bug, ai-studio, gemini-api, gemini-25	13	413	Aug 2025
Google AI studio is unsafe for private data Google AI Studio prompt, generative-ai	5	5.1k	Apr 2025
Request Deletion of Confidential Company Data AI Studio API Free Tier Gemini API ai-studio	0	37	15d